

RIESGOS de las OPERACIONES

En la cumbre de la OTAN no se hizo mucho hincapié en que la Alianza se encuentra sumida en un proceso de transformación, al igual que ocurre en España en el ámbito de la Seguridad y Defensa. En ese proceso destaca un concepto, NEC (siglas en inglés de Capacidad para Trabajar en Red), nombre con el que el Ministerio de Defensa británico de mejorar la efectividad militar mediante un mejor uso de los sistemas de información para disponer de “los datos correctos, en el lugar y momento adecuados... y sólo los justos”. En torno al mismo existen diferencias respecto a su alcance e interpretación, que plantean preguntas como ¿cuál ha sido el camino seguido hasta su adopción? o ¿existen riesgos asociados a su establecimiento?

NEC IMPLICA DESAFÍOS...

El concepto NEC presenta indudables ventajas y responde a las necesidades de un concepto moderno de Seguridad y Defensa. Pero la complejidad del mismo, y su desarrollo en un entorno pluridisciplinar y multinacional, ofrece también importantes desafíos a los que es preciso hacer frente para que su puesta en escena proporcione los frutos deseados.

El reto es importante pues en la filosofía NEC se integran no solamente sensores, sistemas y plataformas, sino

también tecnologías, estructuras de fuerzas, doctrinas, estrategias y múltiples actores, incluyendo la revisión de algunos conceptos ligados a las políticas nacionales de Defensa.

Un primer desafío, generalmente reconocido, es la necesidad de ser interoperables. La realidad muestra que, especialmente en los niveles táctico y operativo, se detecta una evidente falta de interoperabilidad derivada de la existencia de varios modelos de datos, sistemas de información diversos, basados en arquitecturas autónomas y cerradas, configuraciones estáticas, redes punto a punto centradas en plataformas, etc.

A la falta de interoperabilidad se añade la dificultad para compartir información, otro requisito necesario para operar en red. La información debe fluir a todos los niveles, del estratégico al operativo, para poder ofrecer a los diferentes comandantes un mejor y más oportuno conocimiento de la situación, particularmente en escenarios complejos.

Para afrontar estos desafíos debe considerarse que la gestión de la información en red no puede verse en un contexto cerrado, sino abierto a los diferentes niveles de las fuerzas involucradas en las operaciones.

Otro desafío al que enfrentarse se deduce del paso del concepto de gestión local de la información, a gestión global en un entorno de red,

incluyendo la necesidad de disponer de un responsable de la administración integral, capaz de reconfigurar los sistemas de información de forma dinámica, adaptándose a en cada caso a la diversidad de escenarios operativos que puedan surgir.

No menos importante es la necesidad de adaptar las estructuras de fuerzas, procesos, métodos, operaciones, doctrinas a una NEC global, común a los tres Ejércitos y multinacional, teniendo en cuenta que las diferencias son sensibles, en personal y material, dependiendo de cada país en coalición,

La adaptación a los conceptos derivados de NEC requiere imperativamente la implicación de los Estados, incluyendo al tejido industrial que debe jugar un papel principal.

La solución no consiste en adoptar directamente las tecnologías propias de los sistemas civiles, pero tampoco hay que inventar o reinventar. Si NEC se basa en las TIC, será suficiente con adaptar las tecnologías civiles adecuadas, como en los casos de COTS y SCOTS, y buscar los mejores compromisos para desarrollar el resto.

Cuando esto no sea posible, las opciones serán la transferencia de tecnología civil, utilización dual o definición de arquitecturas propias, basadas en componentes modulares, que permitan integrar futuros

NEC MILITARES EN RED

La Network Enable Capacity, más conocida como guerra en red es un concepto que nace al amparo del reciente impulso que han experimentado las tecnologías de la comunicación.

En esencia se concreta en los siguientes fines: el conocimiento en tiempo real de la misma imagen del campo de batalla, cada uno a su nivel, del despliegue de las fuerzas amigas y enemigas; y en el acortamiento de la conocida como ‘kill chain’ o ‘sensor to shooter’, el tiempo que pasa entre la detección y envío de los datos de un objetivo por un sensor, se identifica, se asigna a un arma, se hace fuego y se valoran los daños, un proceso básico para batir objetivos de forma oportuna, especialmente a los que están en movimiento.

Un ejemplo: un avión no tripulado que localiza un lanzacohetes de artillería: la ‘kill chain’ comenzaría con su localización y envío de sus datos de posición e imagen

al puesto de mando, seguiría con la identificación del arma, su asignación a un avión de combate, pieza de artillería u otra arma, cálculo instantáneo de los datos de tiro gracias a las coordenadas transmitidas por el avión no tripulado, fuego y retransmisión de la imagen tras ser alcanzado, para conocer los efectos conseguidos. La guerra en red exige un gran despliegue de sensores tripulados y no tripulados, terrestres,

aéreos y en su caso navales y un conjunto de armas integradas en plataformas también terrestres, aéreas y navales, complementados con un despliegue de comunicaciones capaz de soportar el tráfico de voz, imágenes fijas y en movimiento en tiempo real. A todo este esfuerzo tecnológico y de inversión

hay que añadir la doctrina, procedimientos de empleo y adiestramiento adecuados.

desarrollos, fomentando la interoperabilidad y estandarización de productos y sistemas, impulsando así la innovación.

Y es necesario realizarlo en un marco de estrecha colaboración de todos los actores, lo que supone que Estados e industrias lleven a cabo una acción conjunta y coordinada para determinar las tecnologías clave que aseguren la eficacia operativa, desarrollarlas e integrarlas en los sistemas buscando el mejor compromiso entre operativos, técnicos, industrias y capacidades y objetivos nacionales.

Finalmente un desafío inherente al concepto de Transformación, y por tanto al de NEC, recogido por la propia OTAN, se refiere al cambio cultural asociado a la puesta en marcha de nuevos conceptos en un entorno multinacional, con doctrinas, capacidades, legislaciones diferentes, en un dominio como el de Seguridad y Defensa donde los Estados son soberanos.

... Y TAMBIÉN PROBLEMAS

A las evidentes ventajas, así como a los retos a afrontar, se unen una serie de riesgos que es preciso estimar para tratar de evitarlos o al menos minimizar su impacto o evitar sus efectos.

En un rápido resumen se identifican riesgos inherentes a la seguridad de los sistemas, o al potencial desequilibrio a introducir en los di-

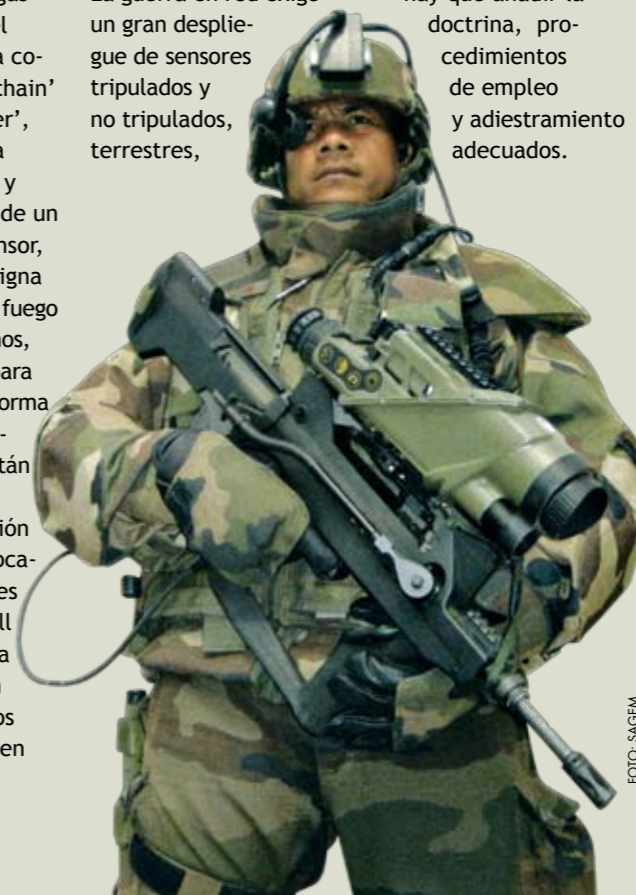


FOTO: SAGEM

ferentes escalones del mando, la posibilidad de saturación de información y sus consecuencias, o el fuerte componente tecnológico, que puede no ser asimilado de igual forma por todos los actores implicados.

Al analizar cada uno de ellos, así como otros no expuestos, se deduce que todos están directamente relacionados con el más importante de los elementos implicados: el factor humano.

El concepto NEC ha sido ya experimentado en varios dominios del sector civil, con otro enfoque y denominación, donde ha podido constatarse que la tecnología es necesaria, imprescindible a veces, pero incrementa la dependencia del citado elemento vital.

Además, tales decisiones inadecuadas no quedarán normalmente limitadas al nivel donde se toman. Por la propia filosofía NEC pueden propagarse por la red global e impactar de una u otra forma en las de otros escalones, provocando la multiplicación de errores.

Como prolongación del anterior se identifica otro riesgo ligado a la acción del mando. Un sistema basado en red favorece la iniciativa individual, al proporcionar hasta el nivel más bajo de las operaciones la información necesaria para desarrollar su acción.

Puesto que, paradójicamente, en este tipo de sistemas la complejidad en la integración aumenta según disminuye el nivel, con un alto

la responsabilidad del mando y favoreciendo la iniciativa individual, con absoluto respeto a las reglas y procedimientos de empleo.

De igual forma debe insistirse en el hecho de que la red es el soporte del flujo de información y el núcleo alrededor del cual se engarza todo el conjunto, pero la toma de decisión corresponde siempre al mando operativo, actuando siempre de acuerdo con las órdenes recibidas.

EPÍLOGO

De lo expuesto puede concluirse que, en términos de operaciones, NEC supone una forma de llevarlas a cabo de forma eficaz, poniendo en relación directa, a cualquier nivel, al conjunto de actores y sistemas implicados, por medio de una red global y virtual de equipos, sensores, plataformas, infraestructuras. .

Pero NEC es un también un noción que engloba doctrinas, organización, formación y personal, junto con conceptos estratégicos, poderes públicos, industrias, etc. Tal complejidad entraña desafíos y riesgos, derivados fundamentalmente de una fuerte dependencia de la información, los sistemas y la tecnología.

El objetivo último es obtener la superioridad en la decisión y esta no se alcanza solamente con tecnología; la dinámica para hacerlo depende fundamentalmente de los procesos y de los hombres. En consecuencia, si la mayor parte de estas dificultades se pueden superar situando al factor humano en el centro de la reflexión, y éste a su vez es un elemento fundamental para alcanzar la superioridad en la decisión, puede concluirse que el concepto NEC podría denominarse 'Centrado en el hombre'. ■

El concepto NEC presenta **indudables ventajas** y responde a las **necesidades** de un concepto moderno de Seguridad y Defensa

Por eso, las modernas organizaciones adoptan estrategias centradas en los individuos, el capital intelectual y la gestión del conocimiento, como factores clave para la optimización de la eficacia, particularmente en entornos en red.

Es lógico deducir que en un contexto de Seguridad y Defensa destaque también el elemento humano, a situar en lugar preferente, base del análisis de los mencionados riesgos.

El peligro de la superabundancia de información normalmente se ve acentuado por la posibilidad de no interpretarla de forma adecuada, lo que conduce a tomar decisiones erróneas, particularmente si se dispone de poco tiempo, algo habitual en operaciones.

grado de incertidumbre, ambas circunstancias pueden dar lugar a que se interprete que se diluye la acción del mando, eventualidad que algunos autores denominan "tendencia al micro mando".

En el lugar opuesto de la jerarquía aparece el riesgo ligado a los administradores de la red virtual quienes pueden también deducir que en determinados momentos ejercen como los verdaderos comandantes de las operaciones.

La forma más adecuada de prevenir tales riesgos es por medio de la formación y entrenamiento adecuados para que todos los actores sean conscientes de que en el sistema debe existir permanentemente el equilibrio en la toma de decisiones, preservando